Method For Utilizing Fragile Watermark For Enhanced Security

Related Applications

The present application is a continuation of co-pending application no. 10/012,703, filed December 7, 2001 (published as US 2002-0061121 A1). The 10/012,703 application is a continuation of application no. 09/433,104, filed November 3, 1999 (now US Patent No. 6,636,615), which is a continuation in part of co-pending application serial number 09/234,780, filed January 20, 1999 (now abandoned), which is a continuation in part of application 60/071,983 filed January 20, 1998.

Field of the Invention

The present invention relates to steganography, and more particularly relates to the use of multiple watermarks to determine the authenticity or history of a particular document or electronic object (e.g., image, motion picture, audio track).

Background of the Invention

Steganographic and digital watermarking technologies are well known. For example see U.S. Patent 5,636,292 and the extensive references cited therein. Also see co-pending patent applications serial number 08/327,426 which was filed 10/21/94 and co-pending application serial number 08/436,134 which was filed 5/8/95.

The technology for inserting digital watermarks in images and the technology for reading or detecting digital watermarks in images is well developed, well known and described in detail in public literature. Furthermore, there are commercially available products which include programs or mechanisms for inserting digital watermarks into images. For example the commercially available and widely used products "Adobe Photoshop" which is marketed by Adobe Corporation of San Jose California and "Corel Draw" program which is marked by Corel Corporation of Ontario Canada, include a facility for inserting digital watermarks into images.

The technology for making high quality copies of documents is widely available. The technical quality of scanners and color printers has been increasing rapidly. Today for a relatively low cost one can purchase a high quality scanner and a high quality color printer. Thus, it is becoming increasingly easy to duplicate documents. The ability to create high quality copies has created a need for technology which can differentiate between original documents and copies of the original.

It is known that watermarks can be used to help differentiate genuine documents from copies. However, the prior art techniques for using digital watermarks to differentiate genuine documents from copies have serious limitations. The present invention is directed to an improved technique for using steganography and digital watermark technology to facilitate differentiating original documents from copies of the original.

The present invention can also be used for various other purposes such as to embed multiple types of information in a single document or to provide watermarks that enable documents to perform special functions. .

Summary of the Invention

With the present invention multiple digital watermarks, each of which has a different character, are embedded in a document. The characters of the two watermarks are chosen so that the watermarks will be affected in different manners by what may subsequently happen to the document.

The detection process or mechanism reads the two digital watermarks and compares their characteristics. While wear and handling may change the characteristics of the individual watermarks, the relationship between the characteristic of the two watermarks will never-the-less give an indication as to whether a document is an original or a copy of an original.

For example according to the present invention two digital watermarks in a document may have different energy levels. The absolute energy level of a digital watermark in an original image may be decreased if a document is subject to wear. Likewise the energy level of the digital watermark in an image may be decreased if an image is scanned and reprinted on a color printer. However, the relationship between the energy level of the two digital watermarks will be different in an image that has been subject to wear and in a reproduced image. Likewise if two digital watermarks are introduced into an image where the bit pattern used to construct the digital watermarks have different patterns, the ratio between the signal to noise ratio of the watermarks will be different in an original subject to wear and in a copy generated by scanning the original and printing the scanned image. Other characteristics of multiple digital watermarks can also be used to differentiate original documents from copies.

In other embodiments, a watermark-independent assessment of wear can be performed, and the results used to aid in differentiating original documents from copies.

Brief Description of the Figures

Figure 1 shows the paths that a document and a copy may follow.

Figures 2A and 2B show a fine grain and a course grain watermark.

Figure 3A and 3B show a geometrically linear and a geometrically random assignment of pixels to a bit in a digital watermark.

Figure 4 illustrates a fourth embodiment of the invention.

Detailed Description

The problem of differentiating an original document from a copy is made more difficult in situations where the original document is subject to being handled, worn, folded and otherwise damaged. Many original documents such as identification documents and currency are extensively handled. The wear to which such documents is subjected

reduces the quality of images on the document and therefore reduces the quality of any information embedded in the document using conventional steganographic techniques.

With the present invention, a number of different watermarks are embedded in a document. Each of the watermarks embedded in the document has a different character. All watermarks are somewhat affected when a document is subjected to wear, and all watermarks are somewhat affected when a document is duplicated by being scanned and reprinted. However, the magnitude of the effect caused by being scanned and reprinted on watermarks with certain characteristics is much greater than the effect on watermarks with different characteristics. Likewise, wear and handling of a document affects watermarks with certain characteristics much more than it affects watermarks with different characteristics.

Thus, if multiple watermarks with different characteristics are inserted into a document, it is possible to differentiate a copy from an original document that has been subjected to wear by examining the ratios of characteristics of the watermarks in the image being examined.

In order to print a document on a color printer, the document is put through a transformation from a color space such as the RGB color space to a different color space such as the CMYK (cyan, magenta, yellow, black) color space. Such transformations are well known. For example see chapter 3 entitled "Color Spaces" in a book entitled "Video Demystified, A handbook for the Digital Engineer," Second Edition, by Keith Jack, published by Harris Semiconductor/ Hightext Publications of San Diego, California, and "The Color PC" by Marc Miller and published by the Hayden Press.

When an image is transformed from one color space to another color space, noise is introduced into the image. Among the reasons for this is the fact that each color space has its own distinctive gamut (or range) of colors. Where the gamut of two color spaces overlap, the conversion from one color space to another color space can in theory be

precise. However, there will be some areas that are in the gamut of one color space but not in the gamut of another color space. Such situations definitely introduce noise into the conversion process. Even in areas that are in the gamut of two color spaces, conversion from one color space to another color space introduces noise because of such things as round off errors. The present invention takes advantage of the fact that if an original is copied and then a copy is printed, the image on the printed copy will have gone through several conversions to which the original will not have been subjected. For example, the conversions to which a copy may be subjected are:

1) a document to RGB conversion (i.e. scanning the document into the computer),
2) a RGB to CMYK conversion,
3) a CMYK to copy conversion (i.e. printing the document).

Any characteristics of the two digital watermarks that will be affected differently by the additional conversion process to which copies are subjected can be used to differentiate copies from an original. Since the two watermarks with different characteristics are affected in a different manner by the additional conversion step, a comparison of the characteristics of the two watermarks in a document being examined will indicate if the document is an original (which has not gone through the additional conversions) or a copy which has gone through the additional conversions. While the characteristics of each watermark will have been changed by wear and by the copying process, the comparison between the characteristics of the two watermarks will still be able to differential a copy from an original.

Four embodiments of the invention are described below. Each of the embodiments utilizes two watermarks in a document. The differences between the two watermarks in the document are as follows:

In the first embodiment:

First watermark: Has fine grain

Second watermark: Has a course grain

In the second embodiment:

First watermark: Has geometrically linear assignment of pixels

Second watermark: Has geometrically random assignment of pixels.

In the third embodiment:

First watermark: Has low power

Second watermark: Has higher power

In the fourth embodiment:

First watermark: uses standard RGB to HSI and HSI to RGB transformations

Second watermark is biased before being transformed from HSI to RGB.

Figure 1 shows the steps to which documents and copies are typically subjected. In the normal course, a document 10 may be subjected to handling and wear 11 resulting in a worn document 10A. Document 10 may also be scanned as illustrated by box 12. The scanning produces a digital image that can be printed, as illustrated by box 13. The printed image may be subjected to handling and wear 14 resulting in a copy 10B. It is noted that the document 10 may also be subject to handling and wear prior to the scanning operation 12. The task to which this invention is directed is the task of differentiating the worn document 10A from the copy 10B.

The document 10 includes an image (not explicitly shown) that has two digital watermarks inserted therein. In the first embodiment of the invention, the first watermark has a fine grain and the second watermark has a course grain. The grain of the two watermarks is illustrated in Figure 2. Figure 2A shows the grain of the first watermark and figure 2B shows the grain of the second watermark. The first watermark uses blocks of 9 pixels (a 3 by 3 block). Each of the pixels in each 9 pixel block has its gray value changed by the same amount. For example Figure 2A shows that the first 9 pixel block has its gray value increase and the second 9 pixel block has its gray value decreased. The amount of increase and the selection of blocks that is increased and decreased is conventional.

As shown in Figure 2B, the grain of the second watermark is in blocks that are 6 pixels by 6 pixels or 36 pixels. All of the pixels in each 36 pixel block are changed by the same amount.

In the original document 10, the two watermarks have power ratios of 1 to 1. After wear and handling, the power of the first watermark will be degraded somewhat more than the power of the second watermark. For example, as illustrated in Figure 1, after document 10 is subjected to handling and wear, a detector which reads the watermarks might find that the power ratio of the water marks is 1 to 2.

If the document 10 is scanned and the resulting digital image is printed to make a copy of the document 10, the ratio of the power of the watermarks will be affected much more than the effect of handling and wear. For example as illustrated in Figure 1, the power ratio of the watermarks may be 1 to 10, thereby allowing one to differentiate the worn original document 10A from the copy 10B.

It is noted that the mechanism for inserting watermarks into an image is well known, as is the technique for reading a watermark and using correlation techniques to determine the signal to noise ratio (i.e. the power) of a watermark.

Figures 3A and 3B show an alternative technique for implementing the present invention. In the second embodiment of the invention, the two watermarks inserted into the image on a document have different patterns of assigning pixels to the bits of the payload represented by the watermark. The first watermark utilizes a geometrically linear assignment of pixels to each bit. For example Figure 3A shows an image that has 500 by 500 pixels. Considering a watermark payload with 50 bits, each bit of the watermark would have 5000 pixels assigned to represent that bit. A linear assignment could have each fifth bit in each row (100 bits per row) and each fifth row (50 rows) assigned to each bit of the watermark. Thus 5000 pixels would be assigned to each bit in a very orderly or linear manner.

In the second watermark the pixels would be assigned to each bit in a random manner as shown in Figure 3B. Each bit in the watermark would still have 5000 assigned bits; however, the pixels would be a random location over the image. Naturally it should be understood that Figure 3A and 3B illustrate how pixels are assigned to one bit of the watermark. The other bits of the watermarks would have pixels assigned in a similar manner.

Similar to the first embodiment of the invention, the watermark with a linear assignment of pixels and the watermark with a random assignment of pixels would be affected differently by handling and wear on the original document than they would be by being scanned and reprinted.

The third embodiment of the invention described herein utilizes watermarks that have different power levels. Handling and wear as contrasted to scanning and printing would affect a watermark with a low power level differently than a watermark with a high power level. Watermarks with different power levels can be inserted into a document in order to practice the present invention utilizing commercially available programs such as Adobe Photoshop or Corel Draw. In the Adobe Photoshop and Corel Draw programs, the power or intensity of the watermark can be adjusted by setting a simple control setting in the program.

The fourth embodiment of the invention introduces different characteristics into two watermarks by modifications made to one of the watermarks during the initial step during which the watermarks are introduced into an image. The operation of the fourth embodiment can be explained as shown in Figure 4. First as illustrated by equation 1 there is a conversion from RGB to HSI as is conventional. This is illustrated by equation 1. As illustrated by equation 2, the first watermark is inserted into the image in a conventional manner by modifying the I value in the HSI representation of the image using the first watermark values (designated as WM1 Δ). A first RGB value designated

RGB(1) is then calculated using a conventional transformation designated T. As indicated by equation 3, the second watermark WM2 is then biased toward a particular color and the biased watermark is then combined with the HSI values and transformed to a second set of RGB values designated RGB(2). Finally as indicated by equation 4, the values RGB(1) and RGB(2) are combined to form the watermarked image designated RGB(F).

The transform used to go from RGB to HSI color space (indicated in equation 1 in Figure 4) can be anyone of a variety of known other techniques. For example, the RGB to HSI conversion can be one of the techniques explained in the above referenced text book such as the following: (which assumes that RGB and Intensity have a value range of 0 to I and that Red equals 0°):

First calculate:

M = max (R,G,B)

m = min (R,G,B)

r = (M-R)/(M-m)

g = (M-G) /M-n)

b = (M-B) / (M-m)

Then calculate I, S, and H as follows:

a) I = (M + M) /2

b) if M = m then S = 0 and H = 180

if I< or = 0.5 then S = (M-m)/(M+m)

if I > 0.5 then S = (M-m) / (2-M-m)

c) if R = M then H = 60 (b-g)

if G = M then H = 60 (2 +r - b)

if B = M then H = 60(4 + g - r)

if H > or = 360 then H = H - 360

if H < 0 then H = H + 360

The first watermark in inserted into the RGB values in a conventional manner by modifying the I value of appropriate pixels so as to combine the watermark Δ values with

HSI values. This is indicated by equation 2 in Figure 4. Next as indicated by equation 3 in Figure 4, the HSI values are converted to RGB values using a transform "T". The transform "T" can be conventional and it can for example be done as follows:

First calculate:

if I < or = 0.5 then M = I (I + S)

if I > 0.5 then M = I + S - IS

m = 2I - M

if S = 0 then R = G = B = I and H = 180°

Then calculate R, G and B as follows:

a) if H < 60 then R = M

if H < 120 then R = m + ((M-m) / ((120- H) / 60))

if H < 240 then R = m

if H < 300 then R = m + ((M - m) / ((H - 240 / 60))

otherwise R = M

b) if H < 60 then G = m + ((M-m)/ (H/60))

if H < 180 then G = M

if H < 240 then G = m + ((M - m) / ((240 - H_ / 60))

otherwise G = m

c) if H < 120 then B = m

if H < 180 then B = m + ((M -m) / ((H-120/60))

if H < 300 then B = M

otherwise B = m + ((M - m) / ((360 - H) / 60))

Next the values which represent a second watermark are used to calculate a second set of RGB values designated RGB2. In order to calculate RGB2, the values of H and S are modified so that they are slightly biased toward a particular color designated H1 and S1 New values for H and S are calculated as follows:

(Note, H1 must be between 0 and 360, S1 must be non-negative and can be between 0 and 1 and X is a value between 0 and 1)

Calculate new values for H and S as follows:

If H > H1 then H = H - (H - H1) x

else H = H + (H1 -H)x

If S > S1 then S= S - (S- S1)x

else S = S +(S1 -S) x

:

Next add the second watermark to the values of HSI and transform these values to the RGB color space as indicated by equation 3 The transformation from HSI color space to RGB color space is done as previously indicated.

Finally as indicated by equation 4 in Figure 4, the final RGB value (designated RGBF) is calculated by combining the values of RGB1 and RGB2. This combination can be done in a variety of known ways.

It is noted that in the above example the difference between the transformation used for the first and the second watermarks involves biasing the values of H and S. Alternatively a wide variety of different changes could also be made. The key to this fourth embodiment of the invention is that in effect a different transformation is used for the first and the second watermarks.

In more sophisticated embodiments, the wear of the document can be independently assessed and used to aid in distinguishing an original from a copy.

There may be cases in which the wear-based degradation to the watermarks in a worn but original document can yield results similar to the scan/print degradation to the watermarks in a crisp copy. For example, consider the case of an original document having watermarks A and B of equal energy, but tailored so that watermark B is more frail and falls-off rapidly in energy when photocopied. On finding a suspect document with a ratio of energy between the two documents in excess of 2:1 (or a commensurate difference in signal-to-noise ratios), a counterfeit may be presumed. However, this ratio

may also result from extreme wear of an original document. See, e.g., the watermark strength v. wear chart of Figs. 5A and 5B for an original document, and the same document after scanning on a 600dpi scanner and printing on a 720 dpi printer. The original document degrades to a watermark energy ratio of 2:1 at point *x*. A crisp copy has the same ratio, resulting in a potential ambiguity.

To distinguish these two cases, the wear of the document can be assessed. Various means can be used to distinguish document wear. One is high frequency content, as can be determined by high pass filtering the document image data, or performing an FFT, DCT, etc. A worn document typically loses some high frequency energy. Another is contrast - a worn document typically loses contrast. Still another is color gamut – a worn document may fade to a less varied gamut. Still another is luminance – the soiling of a document can decrease the overall document brightness. Yet another is physical integrity – a worn document droops when only partially supported. Yet another means is a quick human assessment of wear, with human entry of a corresponding datum into a system (e.g., on a wear scale of 0 to 10, or simply "crisp," "used," or "very worn"). Still other means can similarly be employed.

The wear can be graded on an arbitrary scale, depending on the particular measurement means used. In an illustrative case, wear may range from 0 ("crisp") to 7(extreme). In the Fig. 5 example, the *x* point may be at wear value 5. In distinguishing the documents, a look-up table, microprocessor-implemented algorithm, or other arrangement can be provided that takes as its input the ratio and wear values, and produces outputs, e.g., as follows:

	Wear=0	Wear=1	Wear=2	Wear=3	Wear=4	Wear=5	Wear=6	Wear=7
Ratio = 1.0	Original	Original	Original	Original	Error?	Error?	Error?	Error?
Ratio = 1.25	Original	Original	Original	Original	Original	Error?	Error?	Error?
Ratio = 1.5	Original	Original	Original	Original	Original	Original	Error?	Error?

Ratio = 1.75	Copy	Copy	Original	Original	Original	Original	Original	Error?
Ratio = 2.0	Copy	Copy	Copy	Copy	Original	Original	Original	Original
Ratio = 2.25	Copy	Copy	Copy	Copy	Copy	Original	Original	Original
Ratio = 2.5	Copy	Copy	Copy	Copy	Copy	Copy	Original	Original
Ratio = 2.75	Copy	Copy	Copy	Copy	Copy	Copy	Original	Original
Ratio = 3.0	Copy	Copy	Copy	Copy	Copy	Copy	Copy	Original
Ratio => 3.25	Copy	Copy	Copy	Copy	Copy	Copy	Copy	Copy

(The "Error?" outputs corresponds to cases that should not occur in actual practice, e.g., a very worn document in which the ratio of watermarks is 1.0.)

While four embodiments and a further enhancement of the invention have been shown herein, it should be understood that many other characteristics and attributes of a digital watermark could be used to practice the present invention in addition to the characteristics and attributes described herein. Furthermore other known digital watermarking techniques can be used together with and applied to the digital watermarks used for the present invention. It is also noted that while in the above examples only two watermarks were used; in some situations one could use three, four five or more watermarks. That is, the embodiments of the invention specifically described herein utilize two watermarks. It should be understood that any number of watermarks could be utilized in like manner. Furthermore while the embodiments shown herein utilize two separate watermarks, the two watermarks used to practice the present invention could be combined into one watermark which has a plurality of separate identifiable and measurable characteristics.

Still further, while the invention was particularly illustrated with reference to watermarking that is effected in the pixel domain, the same techniques are likewise applicable to watermarking effected in the DCT, wavelet, or other domain (e.g., as shown in US Patent 5,930,369). Moreover, some documents may include watermarks effected in two different domains (e.g., pixel and DCT).

Still further, the different watermarks can be of entirely different types. For example, one watermark can comprise slight alterations to the image normally printed on a document, and the second can comprise a texture formed on the document substrate, or a background weave or tint pattern – both of which convey watermark data. (Examples of texture-, weave- and tint-based watermarks are shown, e.g., in copending applications 09/074,034 (filed May 6, 1998), 09/127,502 (filed July 31, 1998), 09/151,492 (filed September 11, 1998), patent 5,850,481, and laid-open PCT publication WO 99/53428.

It is noted that while the present invention utilizes multiple watermarks with different characteristics to differentiate original documents from copies of the original, one can also utilizes multiple watermarks with different characteristics for other reasons. Documents may include multiple similar watermarks in addition to the watermarks having different characteristics according to the present invention. As used herein, the term "document" generally refers to a physical entity. However, the same methodologies can also be applied to purely digital images – e.g., to detect losses that an image has suffered through a lossy compression/decompression process such as JPEG or MPEG, color re-balancing, etc., and thereby discern something about the history of a digital image.

It will be recognized that the principles of the invention can be incorporated into an apparatus used at cash registers and other points of sale to assess the genuineness of banknotes, food stamps, coupons, and other documents. Such an apparatus can include a scanning 1D, or stationary 2D image sensor (e.g., CMOS or CCD), and a microprocessor suitably programmed to discern first and second watermarks in image data provided by

the sensor (as well as wear, if desired). (In some cases, a stationary 1D sensor may be employed.) Such apparatus further includes an output device - such as a display screen, indicator light, audible tone, voice synthesizer, or equivalent device - to provide an appraisal of the document's validity based on the sensed information.

A similar apparatus can be provided for use by Customs officials at ports of entry to check merchandise tags, packaging, labels, and other printed indicia associated with clothing, purses, electronic components, software, and other readily-counterfeitable goods, to determine whether the sensed tag/package/label is an original, or a copy. While such a determination may not provide the confidence needed to seize a shipment as counterfeit, it could flag the goods as suspect and needing further inspection and/or forensic analysis.

The idea in each of the foregoing apparatuses is, of course, to provide an indication of possible non-genuineness more reliable than the typical casual and semi-casual human inspection during very fast point-of-sale transactions and other similar high traffic volume situations, where it is unrealistic to expect human observation to be efficient "flaggers" of suspect product and documents.

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the documents (including applications) cited above.

While the present invention has been described with respect to four specific embodiments of the invention, it should be understood that various changes in forma and detail could be made without departing from the spirit and scope of the invention. The scope of the present invention is limited only by the appended claims.